Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 156 (2008) 3122–3138
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Applications to cryptography of twisting commutative algebraic groups

A. Silverberg*

Mathematics Department, University of California, Irvine, CA 92697-3875, USA

Received 25 March 2007; received in revised form 19 September 2007; accepted 7 January 2008
Available online 10 March 2008

Abstract

We give an overview on twisting commutative algebraic groups and applications to discrete log-based cryptography. We explain how discrete log-based cryptography over extension fields can be reduced to cryptography in primitive subgroups. Primitive subgroups in turn are part of a general theory of tensor products of commutative algebraic groups and Galois modules (or twists of commutative algebraic groups), and this underlying mathematical theory can be used to shed light on discrete log-based cryptosystems. We give a number of concrete examples, to illustrate the definitions and results in an explicit way.

Keywords: Discrete log-based cryptography; Commutative algebraic groups; Restriction of scalars; Torus-based cryptography

1. Introduction

In this paper we give a survey on twisting commutative algebraic groups and applications to discrete log-based cryptography. One of our goals will be to explain part of the paper [23] at a more down-to-earth, less technical level, and explain some of its connections to cryptography, in order to make these ideas accessible to a wider audience of mathematicians and cryptographers. We hope that this more general setting will lead to a better understanding of known cryptosystems and their underlying mathematics, and possibly lead to new ideas. We give an overview; see the cited papers for details. In particular, see [23] for most of the results stated in this paper.

A number of cryptosystems, including the Lucas-based [24,36,37,41,42], Gong–Harn [13], XTR [2,20], and $\mathbb{T}_2$ and CEILIDH [27] cryptosystems, and the abelian variety or elliptic curve systems in [26], can be viewed as being based on the idea that when one does discrete log-based cryptography (for either a multiplicative group of a field or an elliptic curve group) over field extensions, one can improve bandwidth efficiency by restricting to a suitable "primitive" subgroup.

Let $\mathbb{F}_q$ denote the finite field with q elements. Discrete log-based cryptography is generally performed using the $\mathbb{F}_q$-points of the multiplicative group $\mathbb{G}_m$, or the $\mathbb{F}_q$-points of an abelian variety A over $\mathbb{F}_q$ (usually an elliptic curve or the Jacobian variety of a hyperelliptic curve). Cryptography over an extension field $\mathbb{F}_{q^n}$ with $n > 1$ uses the groups

$$\mathbb{G}_m(\mathbb{F}_{q^n}) = \mathbb{F}_{q^n}^{\times} = \mathbb{F}_{q^n} - \{0\}$$

* Fax: +1 949 824 7993.
E-mail address: asilverb@math.uci.edu.

0166-218X/$ - see front matter
doi:10.1016/j.dam.2008.01.024

or $A(\mathbb{F}_{q^n})$, where A is an abelian variety over $\mathbb{F}_{q^n}$. The group of $\mathbb{F}_{q^n}$-points of $\mathbb{G}_m$ or A is isomorphic to the group of $\mathbb{F}_q$-points of the Weil restriction of scalars (see Definition 2.2) of $\mathbb{G}_m$ or A from $\mathbb{F}_{q^n}$ down to $\mathbb{F}_q$. So the Weil restriction of scalars arises naturally when doing discrete log-based cryptography over extension fields (see [7,25,5,6,12,9]).

Letting $V = \mathbb{G}_m$ or A, where A is now an abelian variety over the ground field $\mathbb{F}_q$, then $V(\mathbb{F}_{q^n})$ has a natural decomposition (via a homomorphism with "controlled" kernel and cokernel) into a direct product of groups $V_d(\mathbb{F}_q)$, over all divisors d of n (see Proposition 5.3). Thus, when doing finite field or abelian variety cryptography over $\mathbb{F}_{q^n}$, it suffices to consider the subgroups $V_d(\mathbb{F}_q)$ for all divisors d of n. Here, V_d is an algebraic torus over $\mathbb{F}_q$ if $V = \mathbb{G}_m$ and is an abelian variety over $\mathbb{F}_q$ if V is an abelian variety. Over $\mathbb{F}_{q^d}$, V_d is isomorphic to $V^{\varphi(d)}$, where φ is the Euler φ-function, so $\dim(V_d) = \varphi(d)\dim(V)$. When $V = \mathbb{G}_m$, then the group $V_d(\mathbb{F}_q)$ is isomorphic to the subgroup of $\mathbb{F}_{q^d}^{\times}$ of order $\Phi_d(q)$, where $\Phi_d(x) \in \mathbb{Z}[x]$ is the cyclotomic polynomial whose complex roots are the primitive dth roots of unity.

It is useful to view these two settings, multiplicative groups of finite fields and abelian varieties over finite fields, as part of a general framework, as in [23]. Instead of dealing separately with $\mathbb{G}_m$ and A, and only considering finite fields, we will consider the more general setting of commutative algebraic groups over arbitrary fields. This generality allows us to consider the two settings of interest in cryptography, namely $\mathbb{G}_m(\mathbb{F}_{q^n})$ and $A(\mathbb{F}_{q^n})$, simultaneously, and to view them in the same general framework. One point of this paper is to show how the general framework in [23] allows one to recover (known) results that were previously dealt with separately in the two cases. Readers who are uncomfortable with the abstract theory are advised to restrict to the multiplicative group and elliptic curves over finite fields.

Sections 2 and 5 below give an overview of the primitive subgroups and their properties. Section 3 includes general definitions of the twisted commutative algebraic group $\mathcal{I} \otimes_{\mathcal{O}} V$ arising from a commutative algebraic group V and a suitable Galois module $\mathcal{I}$, as given in [23]. Special cases of the varieties $\mathcal{I} \otimes_{\mathcal{O}} V$ include powers, restrictions of scalars, twists of elliptic curves or abelian varieties, and primitive subgroups, including the algebraic tori that arise in torus-based cryptography and the abelian varieties that arise in [26]. In Section 4 we discuss the decomposition of the group rings $\mathbb{Q}[G]$, for G a finite abelian group, that gives rise to the decomposition of the restriction of scalars into primitive subgroups, and work out a concrete example in Section 5.6. In Section 6 on open problems we encourage work on questions of efficiently representing elements of primitive subgroups, and cryptographic security. Interspersed throughout the paper are a number of examples. In particular, we use the cases of quadratic twists of elliptic curves and algebraic tori associated to quadratic extensions to illustrate a number of definitions and properties. See [26,27,29] for additional examples.

Primitive subgroups associated with abelian varieties were discussed in a cryptographic context in [8,26], and have also arisen in work on polarizations on abelian varieties [16], constructing abelian varieties over number fields with Shafarevich–Tate groups of nonsquare order [38], and bounding below the Selmer rank of abelian varieties over dihedral extensions of number fields [22]. See [4,10] for the setting of generalized Jacobians.

Related tensor product constructions were given in [15] (see Proposition 12.7 on p. 205), Section 2 of [31] (when V is an elliptic curve with complex multiplication by $\mathcal{O}$ and $\mathcal{I}$ is a projective $\mathcal{O}$-module with trivial Galois action), [21] (for abelian varieties) and Section 7 of [3] (when V is a group scheme with $\mathcal{O}$-action and $\mathcal{I}$ is a projective $\mathcal{O}$-module with trivial Galois action). In the case of abelian varieties, the restriction of scalars was decomposed into primitive pieces in [6] (see also [5,25]). We note that the relevant parts of [6] hold without change for arbitrary commutative algebraic groups.

As usual, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$ denote the integers, rational numbers, and complex numbers. If R is a commutative ring and G is a finite group, let

$$R[G] := \left\{ \sum_{g \in G} a_g g : a_g \in R \right\}.$$

2. Primitive subgroups

In Definition 2.4 below we will give several equivalent definitions of primitive subgroups. We begin by defining algebraic groups and the Weil restriction of scalars.

Definition 2.1. An **algebraic group** or **group variety** is an algebraic variety V together with a "group operation" morphism $G \times G \to G$ and an "inverse" morphism $G \to G$ with respect to which G is a group. A **homomorphism** of algebraic groups is a morphism of varieties that is also a group homomorphism.

Suppose in this section that V is a commutative algebraic group over a field k, and L is an abelian extension of k of finite degree n. We will view the group law on V multiplicatively. When restricting to examples, this is fine when V is the multiplicative group $\mathbb{G}_m$, but unfortunately is perhaps confusing when V is an elliptic curve, where one normally uses additive notation.

2.1. Restriction of scalars

Definition 2.2. The **restriction of scalars** of V from L down to k, denoted $\mathrm{Res}_k^L(V)$ or $\mathrm{Res}_{L/k}(V)$ (we will use the former notation), is a commutative algebraic group over k along with a homomorphism

$$\eta_{L/k} : \mathrm{Res}_k^L(V) \to V$$

defined over L, with the universal property that for every variety X over k, the map

$$\mathrm{Hom}_k(X, \mathrm{Res}_k^L(V)) \xrightarrow{\sim} \mathrm{Hom}_L(X, V), \quad f \mapsto \eta_{L/k} \circ f \tag{2.1}$$

is an isomorphism.

For every k-algebra A, it follows (by taking $X = \mathrm{Spec}(A)$) that $\eta_{L/k}$ induces an isomorphism $\eta_{L/k} : (\mathrm{Res}_k^L(V))(A) \xrightarrow{\sim} V(A \otimes_k L)$. In particular,

$$(\mathrm{Res}_k^L(V))(k) \cong V(L). \tag{2.2}$$

Further, if $k \subseteq M \subseteq L$ then

$$\mathrm{Res}_k^M(\mathrm{Res}_M^L(V)) = \mathrm{Res}_k^L(V). \tag{2.3}$$

(See Section 1.3 of [40] or Section 3.12 of [39] for background on the restriction of scalars.)

Remark 2.3. More concretely, if V is defined by a system of polynomial equations

$$f_i(x_1, \ldots, x_r) = 0, \quad 1 \le i \le s$$

with coefficients in k (or more generally, L), fix a basis $\{v_1, \ldots, v_n\}$ for L over k, and write $x_i = \sum_{j=1}^n y_{ij} v_j$ with variables y_{ij}. Substitute this into the equations $f_i(x_1, \ldots, x_r) = 0$, expand, and equate coefficients of the basis vectors $\{v_1, \ldots, v_n\}$, to obtain a system of polynomials in the variables $\{y_{ij}\}$ with coefficients in k. The $n \cdot \dim(V)$-dimensional variety over k defined by these equations is $\mathrm{Res}_k^L(V)$.

Next, we give two examples. We will use these examples throughout the paper, as a simple way to illustrate the mathematical definitions and results. See [26,27,29] for other examples.

2.1.1. The multiplicative group and quadratic extensions

Suppose k is a field whose characteristic is not 2, and suppose $D \in k^\times$ is a nonsquare. Let $L = k(\sqrt{D})$, let $G = \mathrm{Gal}(L/k)$, and let σ be the generator of G. It is standard to view the multiplicative group $\mathbb{G}_m$ as the variety in $\mathbb{A}^2$ defined by the equation $xy = 1$, which is the same as identifying $\mathbb{G}_m$ with the nonzero part of the x-line. Then $\mathrm{Res}_k^L(\mathbb{G}_m)$ is the variety R in $\mathbb{A}^3$ defined by the equation $(x_1^2 - Dx_2^2)y = 1$, which is an algebraic group with multiplication $(x_1, x_2, y) \cdot (w_1, w_2, z) = (x_1w_1 + Dx_2w_2, x_1w_2 + x_2w_1, yz)$ and identity element $(x_1, x_2, y) = (1, 0, 1)$. That $\mathrm{Res}_k^L(\mathbb{G}_m) = R$ can be seen as follows. Define

$$\eta_{L/k} : R \to \mathbb{G}_m, \qquad (x_1, x_2, y) \mapsto (x_1 + x_2\sqrt{D}, (x_1 - x_2\sqrt{D})y)$$

(or more simply, $(x_1, x_2, y) \mapsto x_1 + x_2\sqrt{D}$). If X is a variety over k and $\psi \in \mathrm{Hom}_L(X, \mathbb{G}_m)$, define

$$\tilde{\psi} = \left(\frac{\psi + \psi^\sigma}{2}, \frac{\psi - \psi^\sigma}{2\sqrt{D}}, \frac{1}{\psi\psi^\sigma} \right) \in \mathrm{Hom}_k(X, R).$$

It is easy to check that $\eta_{L/k} \circ \tilde{\psi} = \psi$. If $f \in \mathrm{Hom}_k(X, R)$, it is easy to check that $\widetilde{(\eta_{L/k} \circ f)} = f$. It follows that the map $f \mapsto \eta_{L/k} \circ f$ of (2.1) is an isomorphism.

2.1.2. Elliptic curves and quadratic extensions

Suppose $E : y^2 = f(x)$ is an elliptic curve over a field k whose characteristic is not 2, with $\deg(f) = 3$, and suppose $D \in k^\times$ is a nonsquare. Let $L = k(\sqrt{D})$, let $G = \mathrm{Gal}(L/k)$, and let σ be the generator of G. Let $E^{(D)}$ be the elliptic curve $Dy^2 = f(x)$, the quadratic twist of E by D. Define

$$\phi : E \xrightarrow{\sim} E^{(D)}, \qquad (x, y) \mapsto (x, y/\sqrt{D}), \tag{2.4}$$

an isomorphism defined over L. Note that $\phi^\sigma = -\phi$. We claim that $\mathrm{Res}_k^L(E)$ is $(E \times E^{(D)})/T$, where

$$T = \{(P, \phi(P)) \in E \times E^{(D)} : 2P = O\} = \ker(f_0) \cap \ker(2)$$

with $f_0 : E \times E^{(D)} \to E$ the map that sends (P, Q) to $P - \phi^{-1}(Q)$. Here,

$$\eta_{L/k} : (E \times E^{(D)})/T \to E, \qquad (P, Q) \mapsto P + \phi^{-1}(Q).$$

To see that the universal property defining $\mathrm{Res}_k^L(E)$ holds for $(E \times E^{(D)})/T$ with this $\eta_{L/k}$, suppose X is a variety over k and $\psi \in \mathrm{Hom}_L(X, E)$, note that multiplication by 2 induces an isomorphism $[2] : E/E[2] \xrightarrow{\sim} E$, let $\varphi = [2]^{-1} \circ \psi \in \mathrm{Hom}_L(X, E/E[2])$, define

$$\lambda : E/E[2] \to (E \times E^{(D)})/T, \qquad P \mapsto (P, \phi(P)) \bmod T,$$
$$\tilde{\psi} := \lambda \circ \varphi + (\lambda \circ \varphi)^\sigma \in \mathrm{Hom}_k(X, (E \times E^{(D)})/T),$$

and check that $\eta_{L/k} \circ \lambda \circ \varphi = \psi$ and $\eta_{L/k} \circ \lambda^\sigma \circ \varphi^\sigma = 0$, and thus

$$\eta_{L/k} \circ \tilde{\psi} = \psi.$$

We leave as an exercise to check that

$$\widetilde{(\eta_{L/k} \circ f)} = f$$

for every $f \in \mathrm{Hom}_k(X, (E \times E^{(D)})/T)$. It follows that the map $f \mapsto \eta_{L/k} \circ f$ of (2.1) is an isomorphism.

More concretely, one can write down a system of equations for $\mathrm{Res}_k^L(E)$ as follows. If E is $y^2 = x^3 + ax + b$, then substituting $x = x_1 + x_2\sqrt{D}$ and $y = y_1 + y_2\sqrt{D}$ gives a system of 2 equations, in the 4 variables x_1, x_2, y_1, y_2, for the variety $\mathrm{Res}_k^L(E)$:

$$y_1^2 + Dy_2^2 = x_1^3 + 3Dx_1x_2^2 + ax_1 + b,$$
$$2y_1y_2 = 3x_1^2x_2 + Dx_2^3 + ax_2.$$

2.2. Definitions and properties of V_F

As before, L/k is a finite abelian extension and V is a commutative algebraic group over k. For every intermediate field F (i.e., $k \subseteq F \subseteq L$) such that F/k is cyclic, in Definition 2.4 below we will define a commutative algebraic group V_F over k such that, with $d := [F : k]$,

$$\mathrm{Res}_k^L(V) \text{ is isogenous over } k \text{ to } \bigoplus_{\substack{k \subseteq F \subseteq L \\ F/k \text{ cyclic}}} V_F \tag{2.5}$$

via isogenies whose kernels are killed by $[L : k]$,

$$V_F \text{ is isomorphic over } F \text{ to } V^{\varphi(d)} \tag{2.6}$$

(so V_F is a twist of $V^{\varphi(d)}$), and

$$V_F(k) \cong \{\alpha \in V(F) : \mathrm{N}_{F/M}(\alpha) = 1 \text{ for all } k \subseteq M \subsetneq F\}, \tag{2.7}$$

where

$$\mathrm{N}_{F/M}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(F/M)} \sigma(\alpha) \in V(M)$$

and 1 is the identity element of $V(k)$.

Taking k-points, it follows from (2.5) and (2.2) that there are homomorphisms (whose kernel and cokernel are "well-controlled" since those of the isogeny in (2.5) are) between the group $V(L)$ and the direct sum $\bigoplus_F V_F(k)$. It follows from (2.6) that $\dim(V_F) = \varphi(d)\dim(V)$.

We next introduce notation needed for Definition 2.4. Let

$$G := \mathrm{Gal}(L/k).$$

If $g \in G$, then $\eta_{L/k}^g \in \mathrm{Hom}_L(\mathrm{Res}_k^L(V), V)$, and by (2.1) there is a unique $g_{L/k,V} \in \mathrm{End}_k(\mathrm{Res}_k^L(V))$ such that $\eta_{L/k} \circ g_{L/k,V} = \eta_{L/k}^g$. Extend $g \mapsto g_{L/k,V}$ linearly to a ring homomorphism

$$\mathbb{Z}[G] \to \mathrm{End}_k(\mathrm{Res}_k^L(V)). \tag{2.8}$$

For $\alpha \in \mathbb{Z}[G]$, denote its image by

$$\alpha_{L/k,V} \in \mathrm{End}_k(\mathrm{Res}_k^L(V)).$$

On the level of k-points, if $\alpha = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, $v \in (\mathrm{Res}_k^L(V))(k)$, and $(\mathrm{Res}_k^L(V))(k)$ is identified with $V(L)$ as in (2.2), then $\alpha_{L/k,V}(v) = \prod_{g\in G} g(v)^{a_g}$. The map (2.8) is injective if the natural map $\mathbb{Z} \to \mathrm{End}_k(V)$ is injective. For example, the map (2.8) is injective when $V = \mathbb{G}_m$ or an abelian variety A, but is not when V is $\boldsymbol{\mu}_n$ (the kernel of raising to the nth power on $\mathbb{G}_m$) or $A[n]$ (the kernel of multiplication by n on A).

If $k \subseteq M \subseteq F$, let

$$\mathrm{N}_{F/M} := \sum_{h \in \mathrm{Gal}(F/M)} h \in \mathbb{Z}[\mathrm{Gal}(F/M)] \subseteq \mathbb{Z}[\mathrm{Gal}(F/k)].$$

Summing the $\mathrm{Gal}(F/M)$-conjugates of $\eta_{F/M}$ gives a homomorphism

$$\sum_{h \in \mathrm{Gal}(F/M)} \eta_{F/M}^h : \mathrm{Res}_M^F(V) \to V$$

defined over M. Taking Res_k^M and using (2.3) gives a homomorphism

$$R_{F/M/k,V} : \mathrm{Res}_k^F(V) = \mathrm{Res}_k^M(\mathrm{Res}_M^F(V)) \to \mathrm{Res}_k^M(V) \tag{2.9}$$

defined over k. On k-points, $R_{F/M/k,V}$ is the norm map from $V(F)$ to $V(M)$, which sends v to $\prod_{h\in\mathrm{Gal}(F/M)} h(v)$.

There is a natural inclusion

$$\iota_{L/F/k,V} : \mathrm{Res}_k^F(V) \hookrightarrow \mathrm{Res}_k^L(V)$$

as follows. By (2.1) there is a homomorphism $\iota : V \to \mathrm{Res}_F^L(V)$ defined over F such that $\eta_{L/F} \circ \iota = \mathrm{id}_V$ (on F-points, ι is the inclusion $V(F) \subseteq V(L) \cong (\mathrm{Res}_F^L(V))(F)$). The equation $\eta_{L/F} \circ \iota = \mathrm{id}_V$ shows that ι is injective. Applying Res_k^F and (2.3) gives the desired inclusion $\iota_{L/F/k,V}$. We will identify $\mathrm{Res}_k^F(V)$ with its image in $\mathrm{Res}_k^L(V)$. Note that

$$(\mathrm{N}_{F/M})_{F/k,V} \in \mathrm{End}_k(\mathrm{Res}_k^F(V)), \qquad R_{F/M/k,V} \in \mathrm{Hom}_k(\mathrm{Res}_k^F(V), \mathrm{Res}_k^M(V)),$$
$$(\mathrm{N}_{F/M})_{F/k,V} = \iota_{F/M/k,V} \circ R_{F/M/k,V}.$$

On k-points, $(\mathrm{N}_{F/M})_{F/k,V}$ is the map from $V(F)$ to $V(F)$ that sends v to $\prod_{h\in\mathrm{Gal}(F/M)} h(v)$.

Let

$$\Omega_{F/k} := \{\text{fields } M : k \subseteq M \subsetneq F\},$$
$$\Omega'_{F/k} := \{M \in \Omega_{F/k} : [F : M] \text{ is prime}\}.$$

Then every element of $\Omega_{F/k}$ is a subfield of some element of $\Omega'_{F/k}$.

If d is a positive divisor of a positive integer n, let

$$\Psi_{n,d}(x) := \frac{x^n - 1}{\Phi_d(x)} \in \mathbb{Z}[x]$$

(recall that $\Phi_d(x)$ is the dth cyclotomic polynomial) and let

$$\Psi_d(x) := \Psi_{d,d}(x) = \frac{x^d - 1}{\Phi_d(x)} \in \mathbb{Z}[x].$$

We next give several equivalent definitions for the variety

$$V_F \subseteq \mathrm{Res}_k^F(V) \subseteq \mathrm{Res}_k^L(V).$$

Definition 2.4. Suppose V is a commutative algebraic group over k, and F/k is cyclic of degree d. Fix a generator τ of $\mathrm{Gal}(F/k)$, and view $\Phi_d(\tau)$, $\Psi_d(\tau) \in \mathbb{Z}[\mathrm{Gal}(F/k)]$ and $\Phi_d(\tau)_{F/k,V}$, $\Psi_d(\tau)_{F/k,V} \in \mathrm{End}_k(\mathrm{Res}_k^F(V))$. Then:

(i) $V_F = \ker(\Phi_d(\tau)_{F/k,V}) \subseteq \mathrm{Res}_k^F(V)$,
(ii) $V_F = \bigcap_{M\in\Omega_{F/k}} \ker((\mathrm{N}_{F/M})_{F/k,V}) = \bigcap_{M\in\Omega'_{F/k}} \ker((\mathrm{N}_{F/M})_{F/k,V}) \subseteq \mathrm{Res}_k^F(V)$,
(iii) $V_F = \bigcap_{M\in\Omega_{F/k}} \ker(R_{F/M/k,V}) = \bigcap_{M\in\Omega'_{F/k}} \ker(R_{F/M/k,V}) \subseteq \mathrm{Res}_k^F(V)$,
(iv) if $F \subseteq L$, L/k is abelian of degree n, and $\sigma \in G := \mathrm{Gal}(L/k)$ is any element such that $\sigma|_F$ generates $\mathrm{Gal}(F/k)$, then:
  (a) $V_F = (\mathrm{N}_{L/F} \cdot \Psi_d(\sigma))_{L/k,V}(\mathrm{Res}_k^L(V)) \subseteq \mathrm{Res}_k^L(V)$,
  (b) $V_F = \mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V$ as defined in Sections 3 and 4.

(In (ii) and (iii) we adopt the convention that $V_k = V$.)

See [23] for the equivalence of the definitions; see also Proposition 5.1 below. Note that V_F is independent of the choice of L in (iv). Taking (iv) with $L = F$ gives

$$V_F = (\Psi_d(\sigma))_{F/k,V}(\mathrm{Res}_k^F(V)) \subseteq \mathrm{Res}_k^F(V).$$

In [27–29], the primitive subgroup V_F was defined as in (the first part of) Definition 2.4(iii) above. Taking k-points in (ii) or (iii) gives (2.7).

When $k = \mathbb{F}_q$, let $V_d := V_{\mathbb{F}_{q^d}}$.

Next, we continue the examples in Section 2.1.1 and Section 2.1.2. With notation D, L, G, σ, E as in Sections 2.1.1 and 2.1.2, let $F = L$. Then $d = 2$, $\mathrm{N}_{L/F} = 1$, $\Phi_d(\sigma) = \sigma + 1 = \mathrm{N}_{L/k}$, and $\Psi_d(\sigma) = \sigma - 1$.

2.2.1. $(\mathbb{G}_m)_L$ with quadratic L

Let $V = \mathbb{G}_m$. We continue the example in Section 2.1.1. Recall that $\mathrm{Res}_k^L(\mathbb{G}_m)$ is the variety R in Section 2.1.1. The image of σ under (2.8) is $\sigma_{L/k,\mathbb{G}_m} \in \mathrm{End}_k(R)$ defined by $\sigma_{L/k,\mathbb{G}_m}(x_1, x_2, y) = (x_1, -x_2, y)$. Further,

$$\Phi_2(\sigma) = (\mathrm{N}_{L/k})_{L/k,\mathbb{G}_m} = (\sigma + 1)_{L/k,\mathbb{G}_m} : R \to R$$

is given by

$$\left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \mapsto \left(x_1^2 - Dx_2^2, 0, \frac{1}{(x_1^2 - Dx_2^2)^2}\right),$$

$R_{L/k/k,\mathbb{G}_m} : R \to \mathbb{G}_m$ is given by

$$\left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \mapsto \left(x_1^2 - Dx_2^2, \frac{1}{x_1^2 - Dx_2^2}\right),$$

and $(\mathrm{N}_{L/k} \cdot \Psi_2(\sigma))_{L/k,\mathbb{G}_m} = (\sigma - 1)_{L/k,\mathbb{G}_m} : R \to R$ is given by

$$\left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \mapsto \left(\frac{x_1^2 + Dx_2^2}{x_1^2 - Dx_2^2}, \frac{-2x_1x_2}{x_1^2 - Dx_2^2}, 1\right).$$

Then $(\mathbb{G}_m)_L = (\sigma - 1)_{L/k,\mathbb{G}_m}(R) = \ker((\sigma + 1)_{L/k,\mathbb{G}_m})$, and $(\mathbb{G}_m)_L$ is the subvariety of $R \subset \mathbb{A}^3$ defined by $x_1^2 - Dx_2^2 = 1 = y$. In particular, its k-points are the norm one elements of L. In [30], $(\mathbb{G}_m)_L$ is called $\mathbb{T}_{L/k}$, and is called $\mathbb{T}_2$ in [29,30] when the fields are finite.

2.2.2. E_L with elliptic curve E and quadratic L

We continue the example in Section 2.1.2. We saw that $\mathrm{Res}_k^L(E) = (E \times E^{(D)})/T$. The image of σ under (2.8) is

$$\sigma_{L/k,E} \in \mathrm{End}((E \times E^{(D)})/T), \qquad \sigma_{L/k,E}(P, Q) = (P, -Q).$$

The natural inclusions of E and $E^{(D)}$ in $E \times E^{(D)}$ induce injective maps from E and $E^{(D)}$ into $(E \times E^{(D)})/T$. It is now easy to check that the image of $E^{(D)}$ in $(E \times E^{(D)})/T$ is both $\ker((\sigma+1)_{L/k,E})$ and $(\sigma-1)_{L/k,E}((E \times E^{(D)})/T)$. Thus $E_L = E^{(D)}$, by Definition 2.4(i), (ii) and (iii), or (iv)(a).

3. General constructions of $\mathcal{I} \otimes_{\mathcal{O}} V$

In this section we state two definitions of a tensor product $\mathcal{I} \otimes_{\mathcal{O}} V$ that were given in [23], and give some examples. The varieties V_F in Definition 2.4 are special cases of $\mathcal{I} \otimes_{\mathcal{O}} V$, as we will discuss in Section 5. Theorem 3.2 states some useful properties of these tensor product varieties; in particular, Theorem 3.2(ii) motivates the notation $\mathcal{I} \otimes_{\mathcal{O}} V$.

Let k_s denote a separable closure of the field k, and let $G_k = \mathrm{Gal}(k_s/k)$.

From now on, suppose that V is commutative algebraic group over k, $\mathcal{O}$ is a commutative ring, $\mathcal{I}$ is a free $\mathcal{O}$-module of finite rank with a continuous right action of G_k, and there is a ring homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$. We view $\mathcal{O}$ as a free rank one $\mathcal{O}$-module with trivial G_k-action. The reader can choose to restrict to the case $\mathcal{O} = \mathbb{Z}$ for simplicity; an example with $\mathcal{O} \neq \mathbb{Z}$ will appear only in Section 3.1.3.

3.1. Definition and examples of $\mathcal{I} \otimes_{\mathcal{O}} V$

Definition 3.1. Let r be the rank of $\mathcal{I}$ as an $\mathcal{O}$-module, and fix an $\mathcal{O}$-module isomorphism $j : \mathcal{O}^r \xrightarrow{\sim} \mathcal{I}$. Let $c_{\mathcal{I}} \in H^1(k, \mathrm{Aut}_{k_s}(V^r))$ be the image of the homomorphism $(\gamma \mapsto j^{-1} \circ j^{\gamma})$ under the composition

$$\begin{array}{ccccc} H^1(k, \mathrm{GL}_r(\mathcal{O})) & \longrightarrow & H^1(k, \mathrm{Aut}_k(V^r)) & \longrightarrow & H^1(k, \mathrm{Aut}_{k_s}(V^r)) \\ \| & & \| & & \\ \mathrm{Hom}(G_k, \mathrm{GL}_r(\mathcal{O})) & & \mathrm{Hom}(G_k, \mathrm{Aut}_k(V^r)) & & \end{array}$$

induced by the homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$. Let $\mathcal{I} \otimes_{\mathcal{O}} V$ be the twist of V^r by the cocycle $c_{\mathcal{I}}$, i.e., $\mathcal{I} \otimes_{\mathcal{O}} V$ is the unique commutative algebraic group over k with an isomorphism $\phi : V^r \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} V$ defined over k_s such that for every $\gamma \in G_k$,

$$c_{\mathcal{I}}(\gamma) = \phi^{-1} \circ \phi^{\gamma}. \tag{3.1}$$

(See Corollaire to Proposition 5 on p. 131 in Section III-1.3 of [33], or Section 3.1 of [39], for twists of algebraic varieties.)

Note that the twists considered here and in [23] do not include all twists of V in the usual sense; that would require taking elements of $H^1(k_s, \mathrm{Aut}_{k_s}(V^r))$ rather than $H^1(k, \mathrm{Aut}_k(V^r))$.

3.1.1. Powers

Powers of V are a special case of $\mathcal{I} \otimes_{\mathcal{O}} V$, namely, take $\mathcal{I} = \mathbb{Z}^r$ (with trivial Galois action), and let j be the identity map on $\mathbb{Z}^r$. Then the cocycle $c_{\mathcal{I}}$ is trivial, and we can take ϕ to be the identity map on V^r, so $\mathbb{Z}^r \otimes_{\mathbb{Z}} V = V^r$. In particular, $V = \mathbb{Z} \otimes_{\mathbb{Z}} V$.

3.1.2. Restriction of scalars

If L/k is a finite Galois extension with $G = \mathrm{Gal}(L/k)$, then (see Proposition 4.1 of [23])

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}} V = \mathrm{Res}_k^L(V).$$

To see this, define $j : \mathbb{Z}^G \xrightarrow{\sim} \mathbb{Z}[G]$ by $(a_g)_{g\in G} \mapsto \sum_{g\in G} a_g g^{-1}$. By Definition 3.1, j induces an L-isomorphism $\phi : V^G \xrightarrow{\sim} \mathbb{Z}[G] \otimes_{\mathbb{Z}} V$. Composing ϕ^{-1} with the projection $V^G \to V$ onto the component corresponding to the identity element of G gives a homomorphism $\eta_{L/k} : \mathbb{Z}[G] \otimes_{\mathbb{Z}} V \to V$ that satisfies the universal property for $\mathrm{Res}_k^L(V)$.

3.1.3. Twists of abelian varieties

Let $\boldsymbol{\mu}_n$ denote the group of nth roots of unity in $\bar{\mathbb{Q}}$, and let ζ_n denote a generator of $\boldsymbol{\mu}_n$.

Suppose A is an abelian variety over a field k and $\boldsymbol{\mu}_n \hookrightarrow \mathrm{End}(A)$. Suppose $\chi : G_k \to \boldsymbol{\mu}_n$ is a homomorphism. Let $\mathcal{O} = \mathbb{Z}[\zeta_n] \hookrightarrow \mathrm{End}(A)$, and let $\mathcal{I}$ be a free rank one $\mathbb{Z}[\zeta_n]$-module with G_k-action defined by $\alpha^\gamma = \chi(\gamma) \cdot \alpha$ for $\gamma \in G_k$ and $\alpha \in \mathbb{Z}[\zeta_n]$. Then the cocycle $c_{\mathcal{I}}$ of Definition 3.1 is χ^{-1}, and $\mathcal{I} \otimes_{\mathcal{O}} A$ is the twist of A by the character χ^{-1}. In Section 3.1.4, we give details in the case of quadratic twists of elliptic curves (see for example Section X.2 of [35]).

In Sections 3.1.4 and 3.1.5, use the notation in Sections 2.2.1, 2.2.2, 2.1.1 and 2.1.2. Then L/k is quadratic. Let

$$\chi_L : G_k \twoheadrightarrow \{\pm 1\}$$

be the quadratic character that factors through $G = \mathrm{Gal}(L/k)$ and let $\mathcal{I}$ be a free rank one $\mathbb{Z}$-module with G_k-action defined by $a^\gamma = \chi_L(\gamma) \cdot a$ for $a \in \mathcal{I}$ and $\gamma \in G_k$. Fix a generator α of $\mathcal{I}$, and define $j : \mathbb{Z} \xrightarrow{\sim} \mathcal{I}$ by $n \mapsto n\alpha$. For $\gamma \in G_k$ and $n \in \mathbb{Z}$ we have $j^{-1} \circ j^\gamma(n) = \chi_L(\gamma) \cdot n$.

3.1.4. Quadratic twists of elliptic curves

Continuing with the example in Sections 2.2.2 and 2.1.2, and using the above notation, we use Definition 3.1 with $V = E$ to compute $\mathcal{I} \otimes_{\mathbb{Z}} E$. We have $c_{\mathcal{I}}(\gamma) = \chi_L(\gamma) = \phi^{-1} \circ \phi^\gamma$ with the isomorphism $\phi : E \xrightarrow{\sim} E^{(D)}$ of (2.4). By Definition 3.1, $\mathcal{I} \otimes_{\mathbb{Z}} E$ is $E^{(D)}$, the twist of E by the quadratic character χ_L.

3.1.5. Quadratic twists of $\mathbb{G}_m$

Continuing with the example and notation in Sections 2.2.1 and 2.1.1, and using the above notation, we use Definition 3.1 with $V = \mathbb{G}_m$ to compute $\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{G}_m$. Using the variety $(\mathbb{G}_m)_L$ of Section 2.2.1 and the isomorphism $\phi : \mathbb{G}_m \xrightarrow{\sim} (\mathbb{G}_m)_L$ defined by

$$(x, y) \mapsto \left(\frac{x+y}{2}, \frac{x-y}{2\sqrt{D}}, 1\right)$$

(whose inverse is the map $(a, b, 1) \mapsto a + b\sqrt{D}$), we have $c_{\mathcal{I}}(\gamma) = \chi_L(\gamma) = \phi^{-1} \circ \phi^\gamma$. Thus, $\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{G}_m$ is $(\mathbb{G}_m)_L$.

3.2. Properties of $\mathcal{I} \otimes_{\mathcal{O}} V$

The next result gathers together a number of results from [23].

Theorem 3.2. *The variety $\mathcal{I} \otimes_{\mathcal{O}} V$ is a commutative algebraic group over k such that:*

(i) *$\mathcal{I} \otimes_{\mathcal{O}} V$ is functorial in both V and $\mathcal{I}$.*

(ii) *For all commutative k-algebras A and all Galois extensions F of k for which G_F acts trivially on $\mathcal{I}$,*

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(F \otimes_k A) \cong \mathcal{I} \otimes_{\mathcal{O}} (V(F \otimes_k A))$$

and

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(A) \cong (\mathcal{I} \otimes_{\mathcal{O}} (V(F \otimes_k A)))^{\mathrm{Gal}(F/k)},$$

where the right-hand sides are the usual tensor products of $\mathcal{O}$-modules.

(iii) *If W is a commutative algebraic group over k and $\mathcal{J}$ is a free $\mathcal{O}$-module of finite rank with a continuous right action of G_k, then there is a natural G_k-equivariant $\mathcal{O}$-module isomorphism*

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{I},\mathcal{J})\otimes_{\mathcal{O}}\mathrm{Hom}_{k_s}(V,W)\xrightarrow{\sim}\mathrm{Hom}_{k_s}(\mathcal{I}\otimes_{\mathcal{O}}V,\mathcal{J}\otimes_{\mathcal{O}}W) \tag{3.2}$$

that restricts to a homomorphism of $\mathcal{O}$-modules

$$\mathrm{Hom}_{\mathcal{O}[G_k]}(\mathcal{I},\mathcal{J})\otimes_{\mathcal{O}}\mathrm{Hom}_{k}(V,W)\hookrightarrow\mathrm{Hom}_{k}(\mathcal{I}\otimes_{\mathcal{O}}V,\mathcal{J}\otimes_{\mathcal{O}}W).$$

(iv) *If F/k is separable, $\mathcal{J}$ is a free $\mathcal{O}$-module of finite rank with a continuous right action of G_k, and $\mathcal{I}$ and $\mathcal{J}$ are isomorphic as $\mathcal{O}[G_F]$-modules, then the commutative algebraic groups $\mathcal{I}\otimes_{\mathcal{O}}V$ and $\mathcal{J}\otimes_{\mathcal{O}}V$ are isomorphic over F.*

(v) *If F/k is separable and G_F acts trivially on $\mathcal{I}$, then $\mathcal{I}\otimes_{\mathcal{O}}V$ is isomorphic over F to $V^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})}$.*

(vi) *If*

$$0\longrightarrow\mathcal{I}\longrightarrow\mathcal{J}\longrightarrow\mathcal{K}\longrightarrow 0$$

is an exact sequence of free $\mathcal{O}$-modules of finite rank with a continuous right action of G_k, then the induced sequence

$$0\longrightarrow\mathcal{I}\otimes_{\mathcal{O}}V\longrightarrow\mathcal{J}\otimes_{\mathcal{O}}V\longrightarrow\mathcal{K}\otimes_{\mathcal{O}}V\longrightarrow 0$$

is an exact sequence of commutative algebraic groups over k.

(vii) *If $\mathcal{I},\mathcal{J}_1,\ldots,\mathcal{J}_t$ are free $\mathcal{O}$-modules of finite rank with a continuous right action of G_k, and $\mathcal{I}\otimes_{\mathbb{Z}}\mathbb{Q}\cong\oplus_{i=1}^{t}(\mathcal{J}_i\otimes_{\mathbb{Z}}\mathbb{Q})$ as $\mathcal{O}[G_k]$-modules, then*

$$\mathcal{I}\otimes_{\mathcal{O}}V \text{ is } k\text{-isogenous to } \oplus_{i=1}^{t}(\mathcal{J}_i\otimes_{\mathcal{O}}V).$$

Proof. See Lemma 1.3, Theorem 1.4, Corollary 1.7, Corollary 1.9, Theorem 2.1, Lemma 2.3, and Corollary 2.5 of [23]. Note that (vi) and (v) follow from (iv), which follows from (iii), which essentially follows from (i). □

Theorem 3.2 can be used to show (2.5)–(2.7) (see [23]). We show how this is done in Section 5, after defining $\mathbb{Z}[G]_F$.

If $f\in\mathrm{Hom}_{\mathcal{O}}(\mathcal{I},\mathcal{J})$ and $V=W$, let

$$f_V\in\mathrm{Hom}(\mathcal{I}\otimes_{\mathcal{O}}V,\mathcal{J}\otimes_{\mathcal{O}}V) \tag{3.3}$$

denote the image of $f\otimes\mathrm{id}_V$ under (3.2). When $\mathcal{O}=\mathbb{Z}$, $\mathcal{I}=\mathcal{J}=\mathbb{Z}[G]$, $V=W$, and $f\in\mathrm{End}_{\mathbb{Z}[G_k]}(\mathbb{Z}[G])=\mathbb{Z}[G]$, then the map

$$\mathbb{Z}[G]\to\mathrm{End}_k(\mathrm{Res}_k^L(V)),\quad f\mapsto f_V \tag{3.4}$$

is the map (2.8).

3.3. An alternate definition of $\mathcal{I}\otimes_{\mathcal{O}}V$

As in the Appendix to [23], if $\mathcal{O}$ is a commutative noetherian ring, then even if the G_k-module and finitely generated $\mathcal{O}$-module $\mathcal{I}$ is not a free $\mathcal{O}$-module, one can define a tensor product $\mathcal{I}\otimes_{\mathcal{O}}V$ that coincides with the above definition where both make sense, as follows.

Definition 3.3. Take an $\mathcal{O}[G]$-presentation of $\mathcal{I}$, i.e., an exact sequence

$$\mathcal{O}[G]^a\xrightarrow{\psi}\mathcal{O}[G]^b\to\mathcal{I}\to 0 \tag{3.5}$$

of $\mathcal{O}[G]$-modules. Then $\mathcal{I}\otimes_{\mathcal{O}}V=\mathrm{coker}(\psi_V)$.

4. Decomposition of group rings

The decomposition of the restriction of scalars $\mathrm{Res}_k^L(V)$ into primitive subgroups arises from a decomposition of the group ring $\mathbb{Q}[\mathrm{Gal}(L/k)]$ into a direct sum of irreducible rational representations. See [32], especially exercise 13.1.

Suppose G is a finite abelian group. We will consider the group rings $\mathbb{Z}[G]$, $\mathbb{Q}[G]$, and $\mathbb{C}[G]$. Lemma 4.2 gives the decomposition of $\mathbb{Q}[G]$ and some properties of its constituent pieces $\mathbb{Z}[G]_H \otimes_{\mathbb{Z}} \mathbb{Q}$. In Section 5 we will see how to use Lemma 4.2 to obtain the properties of $\mathrm{Res}_k^L(V)$ and its constituent pieces V_F that were stated in Section 2.2.

We begin by decomposing $\mathbb{C}[G]$. Let $\hat{G}$ be the character group of G, i.e., the set of homomorphisms from G to $\mathbb{C}^\times$. For $\chi \in \hat{G}$, let

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\chi(g)g^{-1} = \frac{1}{|G|}\sum_{g\in G}\chi^{-1}(g)g \in \mathbb{C}[G].$$

Then:

- $e_\chi^2 = e_\chi$,
- $e_\chi e_\psi = 0$ if $\chi \neq \psi$,
- $\sum_{\chi\in\hat{G}} e_\chi = 1$ (the identity element of G),
- $e_\chi \mathbb{C}[G] = e_\chi \mathbb{C}$, a one-dimensional $\mathbb{C}$-vector space,
- $\mathbb{C}[G] = \sum_{\chi\in\hat{G}}(e_\chi \cdot \mathbb{C}[G]) = \bigoplus_{\chi\in\hat{G}}(e_\chi \cdot \mathbb{C}[G]) = \bigoplus_{\chi\in\hat{G}} e_\chi \mathbb{C}$.

A problem with decomposing $\mathbb{Q}[G]$ or $\mathbb{Z}[G]$ is that $\chi(g)$ is not necessarily in $\mathbb{Q}$, so the idempotents e_χ are not necessarily in $\mathbb{Q}[G]$. One therefore needs to consider a sum of e_χ's, corresponding to an irreducible rational representation of G.

Lemma 4.1. *Let C_G be the set of subgroups H of G such that G/H is cyclic, let R_G be the set of irreducible rational representations of G, and let X_G be the set of $G_{\mathbb{Q}}$-orbits of $\hat{G}$, where $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then C_G, R_G, and X_G are in natural one-to-one correspondence.*

Proof. If $H \in C_G$, let $Y_H := \{\chi \in \hat{G} : \ker(\chi) = H\} \in X_G$. Conversely, if $Y \in X_G$, let $H_Y := \ker(\chi)$ for any $\chi \in Y$; then $G/H_Y \cong \chi(G)$, a finite, and therefore cyclic, subgroup of $\mathbb{C}^\times$, so $H_Y \in C_G$. If $Y \in X_G$, then $\sum_{\chi\in Y} e_\chi \in \mathbb{Q}[G]$, and the action of G on $\sum_{\chi\in Y}(e_\chi)\mathbb{Q}[G]$ is an irreducible rational representation ρ_Y of G, so $\rho_Y \in R_G$. Conversely, if $\rho \in R_G$, decompose ρ over $\mathbb{C}$ into a direct sum of characters of G. Since ρ is rational and irreducible, this gives a single $G_{\mathbb{Q}}$-orbit Y_ρ of $\hat{G}$. □

If $H \in C_G$, let

$$e_H = \sum_{\chi\in Y_H} e_\chi \in \mathbb{Q}[G].$$

Then:

- $e_H^2 = e_H$,
- $e_{H_1}e_{H_2} = 0$ if $H_1 \neq H_2$, and
- $\sum_{H\in C_G} e_H = 1$.

Let $\mathbb{Q}[G]_H = e_H \cdot \mathbb{Q}[G]$, a simple $\mathbb{Q}[G]$-submodule of $\mathbb{Q}[G]$. Then $\mathbb{Q}[G]_H$ is the unique irreducible rational representation of G contained in $\mathbb{Q}[G]$ whose kernel is H, and

$$\mathbb{Q}[G] = \bigoplus_{H\in C_G}(e_H \cdot \mathbb{Q}[G]) = \bigoplus_{H\in C_G}\mathbb{Q}[G]_H. \tag{4.1}$$

Let

$$\mathbb{Z}[G]_H = \mathbb{Q}[G]_H \cap \mathbb{Z}[G]$$

and let

$$\mathrm{N}_H = \sum_{h\in H} h.$$

Since $\mathbb{Z}[G]_H$ is a submodule of $\mathbb{Z}[G]$, it is a free $\mathbb{Z}$-module.

Lemma 4.2. *Suppose G is a finite abelian group, $H \in C_G$, $\sigma \in G$ is such that σH is a generator of G/H, and $d := |G/H|$. Then:*

(i) $\mathbb{Z}[G]_H = \mathrm{N}_H \cdot \Psi_d(\sigma) \cdot \mathbb{Z}[G] \cong \mathbb{Z}[x]/(\Phi_d(x))$,
(ii) $\mathbb{Z}[G]_H \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{N}_H \cdot \Psi_d(\sigma) \cdot \mathbb{Q}[G] = \mathbb{Q}[G]_H$,
(iii) $\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}[G]_H) = \varphi(d)$,
(iv) $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[G] = \bigoplus_{H \in C_G} (\mathbb{Z}[G]_H \otimes_{\mathbb{Z}} \mathbb{Q})$,
(v) $\mathbb{Z}[G]/\bigoplus_{H \in C_G} \mathbb{Z}[G]_H$ *is killed by* $|G|$.
(vi) *If further G is cyclic of order n and σ generates G, then viewing $\Phi_d(\sigma) \in \mathrm{End}(\mathbb{Z}[G])$ we have*

$$\mathbb{Z}[G]_H = \Psi_{n,d}(\sigma) \cdot \mathbb{Z}[G] = \ker(\Phi_d(\sigma)).$$

Proof. Let $\beta = \mathrm{N}_H \cdot \Psi_d(\sigma)$. For $\chi \in \hat{G}$, if $\ker(\chi) = H$ then $e_\chi \cdot \beta \cdot \mathbb{C}[G] = e_\chi \cdot \mathbb{C} = e_\chi \cdot e_H \cdot \mathbb{C}[G]$, while if $\ker(\chi) \neq H$ then $e_\chi \cdot \beta \cdot \mathbb{C}[G] = 0 = e_\chi \cdot e_H \cdot \mathbb{C}[G]$. It follows that $\beta \cdot \mathbb{C}[G] = e_H \cdot \mathbb{C}[G]$. By linear algebra,

$$\beta \cdot \mathbb{Q}[G] = e_H \cdot \mathbb{Q}[G] = \mathbb{Q}[G]_H. \tag{4.2}$$

By inspection, $\mathrm{N}_H\mathbb{Q}[G] \cap \mathbb{Z}[G] = \mathrm{N}_H\mathbb{Z}[G]$, and it follows that $\mathbb{Z}[G]/\mathrm{N}_H\mathbb{Z}[G]$ is a torsion-free $\mathbb{Z}$-module. The map

$$\pi_H : \mathrm{N}_H\mathbb{Z}[G] \xrightarrow{\sim} \mathbb{Z}[G/H], \qquad \mathrm{N}_H \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g (gH)$$

is an isomorphism of $\mathbb{Z}[G]$-modules that induces an isomorphism

$$\mathrm{N}_H\mathbb{Z}[G]/\beta\mathbb{Z}[G] \xrightarrow{\sim} \mathbb{Z}[G/H]/\Psi_d(\sigma H)\mathbb{Z}[G/H] \cong \mathbb{Z}[x]/(\Psi_d(x)),$$

and the latter is a torsion-free $\mathbb{Z}$-module since $\Psi_d(x)$ is monic. From the exact sequence

$$0 \longrightarrow \mathrm{N}_H\mathbb{Z}[G]/\beta\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]/\beta\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]/\mathrm{N}_H\mathbb{Z}[G] \longrightarrow 0$$

it follows that $\mathbb{Z}[G]/\beta\mathbb{Z}[G]$ is a torsion-free $\mathbb{Z}$-module, and now (4.2) gives that $\beta \cdot \mathbb{Z}[G] = \mathbb{Z}[G]_H$. Further, via π_H,

$$\beta\mathbb{Z}[G] \xrightarrow{\sim} \Psi_d(\sigma H)\mathbb{Z}[G/H] \xrightarrow{\sim} \Psi_d(x)(\mathbb{Z}[x]/(x^d - 1)) \cong \mathbb{Z}[x]/(\Phi_d(x)),$$

and we have (i) and (ii). Since $\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}[x]/(\Phi_d(x))) = \varphi(d)$, we have (iii). Now (iv) follows from (4.1) and (ii). If $\alpha \in \mathbb{Z}[G]$, then

$$|G| \cdot \alpha = \sum_{H \in C_G} e_H |G| \alpha \in \bigoplus_{H \in C_G} \mathbb{Z}[G]_H.$$

Thus

$$|G| \cdot \mathbb{Z}[G] \subseteq \bigoplus_{H \in C_G} \mathbb{Z}[G]_H \subseteq \mathbb{Z}[G] \tag{4.3}$$

and (v) follows.

Suppose G is cyclic of order n with generator σ, and view $\mathbb{Z}[x]/(x^n - 1)$ as a G-module with σ acting as multiplication by x. Since

$$\Psi_{n,d}(x) = (1 + x^d + x^{2d} + \cdots + x^{n-d})\,\Psi_d(x)$$

we have $\Psi_{n,d}(\sigma) = \mathrm{N}_H\,\Psi_d(\sigma)$. By (i), we have $\mathbb{Z}[G]_H = \Psi_{n,d}(\sigma)\mathbb{Z}[G]$. Since the latter is isomorphic to $\Psi_{n,d}(x)(\mathbb{Z}[x]/(x^n - 1))$, which is the kernel of multiplication by $\Phi_d(x)$ in $\mathbb{Z}[x]/(x^n - 1)$, it follows that $\Psi_{n,d}(\sigma)\mathbb{Z}[G]$ is the kernel of multiplication by $\Phi_d(\sigma)$ in $\mathbb{Z}[G]$. □

5. Primitive subgroups, revisited

Suppose that L/k is a finite abelian extension, $G = \mathrm{Gal}(L/k)$, $k \subseteq F \subseteq L$, F/k is cyclic, $d = [F : k]$, and $H = \mathrm{Gal}(L/F)$. Let

$$\mathbb{Z}[G]_F := \mathbb{Z}[G]_H \quad \text{and} \quad \mathbb{Q}[G]_F := \mathbb{Q}[G]_H.$$

Suppose that V is a commutative algebraic group over k. Viewing $\mathbb{Z}[G]_F$ as a G_k-module, then $\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V$ (as defined using Definition 3.1) is a commutative algebraic group over k.

Suppose $k \subseteq M \subseteq F$. Letting

$$R_{F/M/k} : \mathbb{Z}[\mathrm{Gal}(F/k)] \to \mathbb{Z}[\mathrm{Gal}(M/k)]$$

be the natural projection map, then the map

$$R_{F/M/k,V} \in \mathrm{Hom}_k(\mathrm{Res}_k^F(V), \mathrm{Res}_k^M(V))$$

defined in (2.9) is the same as the map $(R_{F/M/k})_V$ obtained from $R_{F/M/k}$ via (3.3) (with $\mathcal{O} = \mathbb{Z}$, $\mathcal{I} = \mathbb{Z}[\mathrm{Gal}(F/k)]$, and $\mathcal{J} = \mathbb{Z}[\mathrm{Gal}(M/k)]$).

Proposition 5.1. *With notation as in Definition 2.4, parts* (a) *and* (b) *of Definition 2.4* (iv) *are equivalent, i.e.,*

$$\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V = \beta_{L/k,V}(\mathrm{Res}_k^L(V)),$$

where $\beta_{L/k,V} = \mathrm{N}_{L/F} \cdot \Psi_d(\sigma) \in \mathbb{Z}[G]$.

Proof. Lemma 4.2(i) gives a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\beta) & \longrightarrow & \mathbb{Z}[G] & \xrightarrow{\beta} & \mathbb{Z}[G]_F & \longrightarrow & 0. \\ & & & & & \searrow^{\beta} & \downarrow & & \\ & & & & & & \mathbb{Z}[G] & & \end{array}$$

Since $\ker(\beta) \subseteq \mathbb{Z}[G]$, $\ker(\beta)$ is torsion-free, and is thus a free $\mathbb{Z}$-module. By Theorem 3.2(vi), there is an induced diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\beta) \otimes_{\mathbb{Z}} V & \longrightarrow & \mathrm{Res}_k^L(V) & \xrightarrow{\beta_V} & \mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V & \longrightarrow & 0 \\ & & & & & \searrow^{\beta_V} & \downarrow & & \\ & & & & & & \mathrm{Res}_k^L(V) & & \end{array}$$

which shows that $\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V = \beta_V(\mathrm{Res}_k^L(V)) = \beta_{L/k,V}(\mathrm{Res}_k^L(V))$. □

We can now show (2.6) and (2.5).

Proposition 5.2. *V_F is isomorphic over F to $V^{\varphi(d)}$.*

Proof. Since $\mathbb{Z}[G]_F$ is a free $\mathbb{Z}$-module of rank $\varphi(d)$ and G_F acts trivially on $\mathbb{Q}[G]_F$, we have $\mathbb{Z}[G]_F \cong \mathbb{Z}^{\varphi(d)}$ as $\mathbb{Z}[G_F]$-modules. The result now follows from Theorem 3.2(v).

Proposition 5.3. *The algebraic varieties* $\mathrm{Res}_k^L(V)$ *and* $\bigoplus_{\substack{k \subseteq F \subseteq L \\ F/k \text{ cyclic}}} V_F$ *are k-isogenous, via isogenies whose kernels are killed by $|G|$.*

Proof. Apply Lemma 4.2(iv) and (v) and Theorem 3.2(vii) with $\mathcal{O} = \mathbb{Z}$, $\mathcal{I} = \mathbb{Z}[G]$, and $\{\mathcal{J}_i\} = \{\mathbb{Z}[G]_F\}$. The inclusions (4.3) induce a sequence of isogenies

$$\mathrm{Res}_k^L(V) \to \bigoplus_{\substack{k \subseteq F \subseteq L \\ F/k \text{ cyclic}}} V_F \to \mathrm{Res}_k^L(V)$$

whose composition is raising to the power $|G|$. □

Suppose G is generated by $\sigma, g_2, \ldots, g_a$, where $g_2, \ldots, g_a \in H$. Then (3.5) with $\mathcal{O} = \mathbb{Z}$ and $\mathcal{I} = \mathbb{Z}[G]_F$ can be taken to be

$$\mathbb{Z}[G]^a \to \mathbb{Z}[G] \to \mathbb{Z}[G]_F \to 0,$$

where the first map is defined by $(\alpha_1, \ldots, \alpha_a) \mapsto \alpha_1 \Phi_d(\sigma) + \sum_{i=2}^{a} \alpha_i (g_i - 1)$ and the second is multiplication by $\mathrm{N}_{L/F}\, \Psi_d(\sigma)$.

Note that $\Psi_1(x) = 1$ and $\Phi_1(x) = x - 1$, so $\mathbb{Z}[G]_k = N_{L/k} \cdot \mathbb{Z}$, a free rank one $\mathbb{Z}$-module with trivial Galois action, and

$$V_k = V = \mathbb{Z}[G]_k \otimes_{\mathbb{Z}} V = \ker((0)_{k/k,V}) = (\mathrm{N}_{L/k})_V(\mathrm{Res}_k^L(V)).$$

In the following subsections we give some special cases of primitive subgroups.

5.1. Trace zero subgroups

Suppose $d = [F : k]$ is prime. Then (by Definition 2.4(ii) or (iii)) V_F is the norm one subgroup of $\mathrm{Res}_k^F(V)$ if the group law on V is viewed multiplicatively, and is the trace zero subgroup when the group law is viewed additively. Further, $\mathrm{Res}_k^F(V)$ is k-isogenous to $V \times V_F$.

Trace zero subgroups of the restriction of scalars for abelian varieties appear in [8,19].

5.2. Decomposition of $\mathrm{Res}_k^L(\mathbb{G}_m)$

Continuing the example in Section 2.1.1, where L/k is quadratic and $\mathrm{Res}_k^L(\mathbb{G}_m) = R \subset \mathbb{A}^3$, we can give the decomposition of $\mathrm{Res}_k^L(\mathbb{G}_m)$ into $\mathbb{G}_m \times (\mathbb{G}_m)_L$ (up to isogeny) explicitly. The homomorphism

$$\mathbb{G}_m \times (\mathbb{G}_m)_L \to \mathrm{Res}_k^L(\mathbb{G}_m), \qquad ((x, y), (a, b, 1)) \mapsto (xa, xb, y^2)$$

has kernel $\{((1, 1), (1, 0, 1)), ((-1, -1), (-1, 0, 1))\}$ of order 2. Composing, in either order, with the homomorphism

$$\mathrm{Res}_k^L(\mathbb{G}_m) \to \mathbb{G}_m \times (\mathbb{G}_m)_L, \qquad (x_1, x_2, y) \mapsto ((y^{-1}, y), ((x_1^2 + Dx_2^2)y, 2x_1x_2y, 1))$$

gives the squaring map.

5.3. Quadratic twists of elliptic curves

Quadratic twists of elliptic curves are examples of both twists of abelian varieties and primitive (in fact, trace zero) subgroups. We continue with the example and notation of Section 3.1.4. Then

$$\mathbb{Z}[G]_k = \mathrm{N}_{L/k}\, \Psi_1(\sigma)\mathbb{Z}[G] = (\sigma + 1)\mathbb{Z} = e_G\mathbb{Q}[G] \cap \mathbb{Z}[G],$$
$$\mathbb{Z}[G]_L = \Psi_2(\sigma)\mathbb{Z}[G] = (\sigma - 1)\mathbb{Z} = e_{\{1\}}\mathbb{Q}[G] \cap \mathbb{Z}[G],$$

free rank one $\mathbb{Z}$-modules, and G_k-modules with $\gamma \in G_k$ acting on $\mathbb{Z}[G]_L$ (resp., $\mathbb{Z}[G]_k$) as multiplication by $\chi_L(\gamma) \in \{\pm 1\}$ (resp., trivially). (Note that $e_G = e_{\chi_0}$ with χ_0 the trivial character, and $e_{\{1\}} = e_{\chi_1}$ with $\chi_1(\sigma) = -1$.)

We saw in Section 3.1.4 that $\mathbb{Z}[G]_L \otimes_{\mathbb{Z}} E = E^{(D)}$. Similarly, $\mathbb{Z}[G]_k \otimes_{\mathbb{Z}} E = E$.

Next we check that Definition 3.3 gives the same answer for $\mathbb{Z}[G]_L \otimes_{\mathbb{Z}} E$. Consider the presentation

$$\mathbb{Z}[G] \xrightarrow{\sigma+1} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G]_L \longrightarrow 0.$$

Since the sequence

$$(E \times E^{(D)})/T \xrightarrow{(\sigma+1)_E} (E \times E^{(D)})/T \xrightarrow{(\sigma-1)_E} E^{(D)} \longrightarrow 0$$

is exact, there is a natural identification of $E^{(D)}$ with $\mathrm{coker}((\sigma + 1)_E)$, as desired.

Similarly, considering

$$(E \times E^{(D)})/T \xrightarrow{(\sigma-1)_E} (E \times E^{(D)})/T \xrightarrow{(\sigma+1)_E} E \longrightarrow 0$$

identifies E with $\mathrm{coker}((\sigma - 1)_E)$, as desired.

To summarize,

$$\begin{aligned} E_k &= E = \ker((\sigma-1)_E) = \operatorname{coker}((\sigma-1)_E) \\ &= (\sigma+1)_E((E\times E^{(D)})/T) = \mathbb{Z}[G]_k \otimes_{\mathbb{Z}} E, \\ E_L &= E^{(D)} = \ker((\sigma+1)_E) = \operatorname{coker}((\sigma+1)_E) \\ &= (\sigma-1)_E((E\times E^{(D)})/T) = \mathbb{Z}[G]_L \otimes_{\mathbb{Z}} E. \end{aligned}$$

The maps

$$\mathbb{Z}[G]_k \times \mathbb{Z}[G]_L \hookrightarrow \mathbb{Z}[G] \to \mathbb{Z}[G]_k \times \mathbb{Z}[G]_L,$$

where the right-hand map is $\alpha \mapsto ((1+\sigma)\alpha, (1-\sigma)\alpha)$ so the composition is multiplication by 2, induce isogenies

$$E_k \times E_L = E \times E^{(D)} \twoheadrightarrow \operatorname{Res}^L_k(E) = (E\times E^{(D)})/T \twoheadrightarrow E \times E^{(D)},$$

where the left isogeny is the natural quotient map and the right isogeny and the composition are multiplication by 2.

5.4. Algebraic tori

In this section, $V = \mathbb{G}_m$.

Proposition 5.4. *Suppose $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$, d is a divisor of n, and $F = \mathbb{F}_{q^d}$. Then:*

(i) $(\mathbb{G}_m)_F(k) \subseteq F^\times$,
(ii) *the group $(\mathbb{G}_m)_F(k)$ is isomorphic to the subgroup of $F^\times$ of order $\Phi_d(q)$,*
(iii) *if $v \in (\mathbb{G}_m)_F(k) \subseteq F^\times$ and v has prime order not dividing d, then for all proper intermediate fields M (i.e., $k \subseteq M \subsetneq F$), we have $v \notin M$.*

Proof. Part (i) follows from Definition 2.4. If $\sigma \in G = \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is the map $x \mapsto x^q$, then the map

$$\mathbb{Z}[G] \to \operatorname{End}_k(\operatorname{Res}^L_k(\mathbb{G}_m))$$

of (3.4) or (2.8) sends $\sum_{i=0}^{n-1} a_i\sigma^i$ to the map that takes v to $v^{\sum a_i q^i}$. Further,

$$(\mathbb{G}_m)_F(\mathbb{F}_q) = \ker(\Phi_d(\sigma)_{L/k,\mathbb{G}_m}) = \ker(v \mapsto v^{\Phi_d(q)}),$$

which is the subgroup of $\mathbb{F}_{q^d}^\times$ (and of $\mathbb{F}_{q^n}^\times$) of order $\Phi_d(q)$. For (iii), see Lemma 1 of [1]. □

Note that if $\mathcal{I}$ is a free $\mathbb{Z}$-module of finite rank with a continuous right action of G_k, then $\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{G}_m$ is the algebraic torus whose character module

$$\operatorname{Hom}(\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{G}_m, \mathbb{G}_m)$$

is $\operatorname{Hom}(\mathcal{I}, \mathbb{Z})$ (see Example 6 in Section 3.4 of [39] or Corollary 1.10 of [23]).

5.5. Algebraic tori over finite fields

The primitive subgroup $(\mathbb{G}_m)_{\mathbb{F}_{q^d}}$ was denoted $\mathbb{T}_d$ in [27–30].

Write $(\mathbb{G}_m)_d := (\mathbb{G}_m)_F$ with $F = \mathbb{F}_{q^d}$. By (2.5) and (2.2), $\mathbb{F}_{q^n}^\times$ can be viewed as "almost isomorphic" to $\bigoplus_{d|n}(\mathbb{G}_m)_d(\mathbb{F}_q)$, and therefore cryptography in $\mathbb{F}_{q^n}^\times$ can be reduced to cryptography in primitive subgroups $(\mathbb{G}_m)_d(\mathbb{F}_q)$ for the divisors d of n. Proposition 5.4(i) implies that attacks (e.g., index calculus attacks) on the discrete log problem in $\mathbb{F}_{q^d}^\times$ give attacks on the discrete log problem in $(\mathbb{G}_m)_d(\mathbb{F}_q)$. Proposition 5.4(iii) tells us that to attack the primitive subgroup $(\mathbb{G}_m)_d(\mathbb{F}_q)$ via an attack that requires using the full multiplicative group of a finite field, no proper subfield of $\mathbb{F}_{q^d}$ suffices. It is in this sense that the subgroup $(\mathbb{G}_m)_n(\mathbb{F}_q)$ of $\mathbb{F}_{q^n}^\times$ $(= \mathbb{G}_m(\mathbb{F}_{q^n}))$ of order $\Phi_n(q)$ is often thought of as the most cryptographically secure primitive subgroup. More generally, one can argue that when V is a commutative algebraic group over $\mathbb{F}_q$, then it makes sense to think of $V_n(\mathbb{F}_q)$ as the most cryptographically secure primitive subgroup of $V(\mathbb{F}_{q^n})$.

5.6. An example with $n = 6$

Suppose G is a cyclic group of order 6. For $d = 2, 3$, let H_d denote the subgroup of G of index d (and order $6/d$). Then

$$\mathbb{Q}[G] = \mathbb{Q}[G]_G \oplus \mathbb{Q}[G]_{H_2} \oplus \mathbb{Q}[G]_{H_3} \oplus \mathbb{Q}[G]_1,$$
$$\dim_{\mathbb{Q}}(\mathbb{Q}[G]_G) = \varphi(1) = 1 = \varphi(2) = \dim_{\mathbb{Q}}(\mathbb{Q}[G]_{H_2}),$$
$$\dim_{\mathbb{Q}}(\mathbb{Q}[G]_{H_3}) = \varphi(3) = 2 = \varphi(6) = \dim_{\mathbb{Q}}(\mathbb{Q}[G]_1).$$

Let $\zeta_6 = (1 + \sqrt{-3})/2$ and $\zeta_3 = \zeta_6^2 = (-1 + \sqrt{-3})/2$. Then

$$\mathbb{Q}[G]_G = e_G \cdot \mathbb{Q} = e_G \cdot \mathbb{Q}[G] = \Psi_{6,1}(\sigma)\mathbb{Q}[G],$$

where $e_G = \frac{1}{6}(1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4 + \sigma^5) = \frac{1}{6}\Psi_{6,1}(\sigma)$;

$$\mathbb{Q}[G]_{H_2} = e_{H_2} \cdot \mathbb{Q} = e_{H_2} \cdot \mathbb{Q}[G] = \Psi_{6,2}(\sigma)\mathbb{Q}[G],$$

where $e_{H_2} = \frac{1}{6}(1 - \sigma + \sigma^2 - \sigma^3 + \sigma^4 - \sigma^5) = -\frac{1}{6}\Psi_{6,2}(\sigma)$;

$$\mathbb{Q}[G]_{H_3} = e_{H_3} \cdot \mathbb{Q}[G] = \Psi_{6,3}(\sigma)\mathbb{Q}[G],$$

where $e_{H_3} = e_{\chi_3} + e_{\chi_3^2} =$

$$\frac{1}{6}[(1 + \zeta_3\sigma + \zeta_3^2\sigma^2 + \sigma^3 + \zeta_3\sigma^4 + \zeta_3^2\sigma^5) + (1 + \zeta_3^2\sigma + \zeta_3\sigma^2 + \sigma^3 + \zeta_3^2\sigma^4 + \zeta_3\sigma^5)]$$
$$= \frac{1}{6}(2 - \sigma - \sigma^2 + 2\sigma^3 - \sigma^4 - \sigma^5) = -\frac{1}{6}\Psi_{6,3}(\sigma)(\sigma + 2);$$
$$\mathbb{Q}[G]_1 = e_1 \cdot \mathbb{Q}[G] = \Psi_{6,6}(\sigma)\mathbb{Q}[G],$$

where $e_1 = e_{\chi_6} + e_{\chi_6^{-1}} =$

$$\frac{1}{6}[(1 + \zeta_6\sigma + \zeta_6^2\sigma^2 - \sigma^3 - \zeta_6\sigma^4 - \zeta_6^2\sigma^5) + (1 + \zeta_6^{-1}\sigma + \zeta_6^{-2}\sigma^2 - \sigma^3 - \zeta_6^{-1}\sigma^4 - \zeta_6^{-2}\sigma^5)]$$
$$= \frac{1}{6}(2 + \sigma - \sigma^2 - 2\sigma^3 - \sigma^4 + \sigma^5) = \frac{1}{6}\Psi_{6,6}(\sigma)(\sigma - 2).$$

Then

$$\mathbb{Z}[G]_G = \Psi_{6,1}(\sigma)\mathbb{Z}[G] = (1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4 + \sigma^5)\mathbb{Z}[G] = \ker(\sigma - 1),$$
$$\mathbb{Z}[G]_{H_2} = \Psi_{6,2}(\sigma)\mathbb{Z}[G] = (-1 + \sigma - \sigma^2 + \sigma^3 - \sigma^4 + \sigma^5)\mathbb{Z}[G] = \ker(\sigma + 1),$$
$$\mathbb{Z}[G]_{H_3} = \Psi_{6,3}(\sigma)\mathbb{Z}[G] = (-1 + \sigma - \sigma^3 + \sigma^4)\mathbb{Z}[G] = \ker(\sigma^2 + \sigma + 1),$$
$$\mathbb{Z}[G]_{\{1\}} = \Psi_{6,6}(\sigma)\mathbb{Z}[G] = (-1 - \sigma + \sigma^3 + \sigma^4)\mathbb{Z}[G] = \ker(\sigma^2 - \sigma + 1).$$

(The fact that $\sigma \pm 2$ is invertible in $\mathbb{Q}[G]$ follows from the fact that, after extending χ to a ring homomorphism $\chi : \mathbb{C}[G] \to \mathbb{C}$, then $\alpha \in \mathbb{Q}[G]$ is a unit if and only if $\chi(\alpha) \neq 0$ for all $\chi \in \hat{G}$.)

If V is a commutative algebraic group over a field k and L is a cyclic degree 6 extension of k, for $d = 2, 3$ let F_d denote the degree d extension of k in L and let $G = \mathrm{Gal}(L/k)$. Then

$$\mathbb{Z}[G]_{F_d} = \mathbb{Z}[G]_{H_d} = \ker(\mathrm{N}_{F_d/k}),$$
$$\mathbb{Z}[G]_L = \mathbb{Z}[G]_{\{1\}} = \ker(\mathrm{N}_{L/F_2}) \cap \ker(\mathrm{N}_{L/F_3}),$$

$V_k = V$, and V_{F_2} is the quadratic twist of V with respect to F_2.

If $k = \mathbb{F}_q$, then $V_L = \ker(q^2 - q + 1) = \ker(\Phi_6(q))$, the subgroup of $\mathbb{F}_{q^6}^{\times}$ of order $\Phi_6(q)$. The cryptosystem CEILIDH [27] is based on this variety, while XTR is based on a quotient of V_L by an action of the symmetric group S_3 (see [27–30]).

6. Open questions and future directions

To do efficient discrete log cryptography in $V(\mathbb{F}_{q^n})$, where V is a commutative algebraic group over $\mathbb{F}_q$, we saw above that one can reduce to considering the subgroups $V_d(\mathbb{F}_q)$, where d is a divisor of n and V_d is V_F with $F = \mathbb{F}_{q^d}$. It makes sense to think of V_n as the most cryptographically secure of the subvarieties V_d, thereby reducing to the case of V_n. Since $\dim(V_n) = \varphi(n)\dim(V)$, in the case where $\dim(V) = 1$ (let us restrict to that case), to obtain the greatest efficiency one would like to represent the elements of $V_n(\mathbb{F}_q)$ using only $\varphi(n)$ elements of $\mathbb{F}_q$. In other words, one would like a low degree compression map $V_n \dashrightarrow \mathbb{A}^{\varphi(n)}$ defined over $\mathbb{F}_q$, where $\mathbb{A}^r$ is affine space of dimension r, along with an efficiently computable decompression function. (We allow the compression and decompression maps to be rational maps, defined only on a Zariski open subset.)

This is done in [26] when V is an elliptic curve E and $n = 3$ or 5, with morphisms $E_n - \{0\} \to \mathbb{A}^{\varphi(n)}$ of degree 8 and 54, respectively (for $n = 2$ or 1, it is easy to do with a degree 2 map). For larger primes n, it is not known how to efficiently decompress elements of $\mathbb{F}_q^{\varphi(n)}$ (the method in [26,34] gives a compression function for which the degree has not been computed, and for which no efficient decompression algorithm is known).

When $V = \mathbb{G}_m$, a trace map is used to give a degree 2 morphism $(\mathbb{G}_m)_n \to \mathbb{A}^{\varphi(n)}$ when $n = 2$ in [24,36,37,41,42] and a degree 6 map when $n = 6$ in [2,20] (for a degree 3 map using 2 symmetric functions when $n = 3$, see [13]). When $V = \mathbb{G}_m$, a degree 1 map (birational isomorphism) $(\mathbb{G}_m)_n \dashrightarrow \mathbb{A}^{\varphi(n)}$ is given in [27] when $n = 2$ or 6. Explicitly (see [27,29]), for $n = 2$ we have

$$(\mathbb{G}_m)_2 \dashrightarrow \mathbb{A}^1, \qquad (a, b, 1) \mapsto \frac{1+a}{b},$$

with inverse map $\alpha \mapsto (\frac{\alpha^2+D}{\alpha^2-D}, \frac{2\alpha}{\alpha^2-D}, 1)$. Via this map, the group law on $(\mathbb{G}_m)_2$ induces an operation $\alpha * \beta = (\alpha\beta + D)/(\alpha + \beta)$ on (most of) $\mathbb{A}^1$ (undefined where $\alpha = -\beta$).

According to Voskresenskiĭ [39], when $V = \mathbb{G}_m$ one should (at least generically) expect a degree 1 map for each positive integer n, i.e., a birational isomorphism between $(\mathbb{G}_m)_n$ and $\mathbb{A}^{\varphi(n)}$ defined over k. (Conjectures that certain symmetric functions should give dominant maps of low degree were given in [1], but counterexamples to these conjectures were then given in [27].) The next interesting case (because $n/\varphi(n)$, which measures the security per bit, is larger than for the case $n = 6$) is when $n = 30$. The rationality of the algebraic torus $(\mathbb{G}_m)_{30}$ is an open question (in characteristic zero, and over finite fields, for example).

Another question that deserves more research is the security of cryptosystems based on primitive subgroups V_n, or the essentially equivalent question of the security of discrete log cryptography over extension fields $\mathbb{F}_{q^n}$ when $n > 1$. In the abelian variety (or elliptic curve) case this is studied in [11], while the $\mathbb{G}_m$ case is studied in [14]. In addition, Joux et al. [17,18] recently obtained variants of the function field and number field sieve that have implications for the security of the discrete log problem for abelian varieties in low characteristic, and for $(\mathbb{G}_m)_{30}$ over $\mathbb{F}_q$ when, for example, q is a 32-bit prime. We encourage further study of the security of cryptosystems based on primitive subgroups.

We also raise the question of finding other applications for varieties $\mathcal{I} \otimes_{\mathcal{O}} V$, in cryptography or elsewhere, including considering other group varieties V and/or other G_k-modules $\mathcal{I}$.

Acknowledgements

The author was supported by NSA grant H98230-07-1-0039. I thank Karl Rubin for help with the paper, and one of the referees for helpful comments.

References

[1] W. Bosma, J. Hutton, E.R. Verheul, Looking beyond XTR, in: Advances in Cryptology — Asiacrypt 2002, in: Lect. Notes in Comp. Sci., vol. 2501, Springer, Berlin, 2002, pp. 46–63.

[2] A.E. Brouwer, R. Pellikaan, E.R. Verheul, Doing more with fewer bits, in: Advances in Cryptology — Asiacrypt '99, in: Lect. Notes in Comp. Sci., vol. 1716, Springer, Berlin, 1999, pp. 321–332.

[3] B. Conrad, Gross–Zagier revisited, in: Heegner points and Rankin L-series, in: Math. Sci. Res. Inst. Pub., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 67–163.

[4] I. Déchène, Generalized Jacobians in cryptography, Ph.D. Thesis, McGill University, 2005. http://www.math.uwaterloo.ca/~idechene/Dechene_thesis.pdf.
[5] C. Diem, A study on theoretical and practical aspects of Weil-restrictions of varieties, Dissertation, 2001. http://www.math.uni-leipzig.de/~diem/dissertation_diem.dvi.
[6] C. Diem, N. Naumann, On the structure of Weil restrictions of abelian varieties, J. Ramanujan Math. Soc. 18 (2003) 153–174.
[7] G. Frey, How to disguise an elliptic curve (Weil descent), lecture at ECC '98. http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps.
[8] G. Frey, Applications of arithmetical geometry to cryptographic constructions, in: D. Jungnickel, H. Niederreiter (Eds.), Finite fields and applications, Augsburg, 1999, Springer, Berlin, 2001, pp. 128–161.
[9] S.D. Galbraith, F. Hess, N.P. Smart, Extending the GHS Weil descent attack, in: L. Knudsen (Ed.), Advances in Cryptology — EUROCRYPT 2002, in: Lect. Notes in Comp. Sci., vol. 2332, Springer, Berlin, 2002, pp. 29–44.
[10] S.D. Galbraith, B.A. Smith, Discrete logarithms in generalized Jacobians, preprint. http://arxiv.org/abs/math/0610073.
[11] P. Gaudry, Index calculus for abelian varieties and the elliptic curve discrete logarithm problem, preprint, October 26, 2004 version.
[12] P. Gaudry, F. Hess, N.P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, J. Cryptology 15 (2002) 19–46.
[13] G. Gong, L. Harn, Public-key cryptosystems based on cubic finite field extensions, IEEE Trans. Inform. Theory 45 (1999) 2601–2605.
[14] R. Granger, F. Vercauteren, On the discrete logarithm problem on algebraic tori, in: V. Shoup (Ed.), Advances in Cryptology — CRYPTO 2005, in: Lect. Notes in Comp. Sci., vol. 3621, Springer, Berlin, 2005, pp. 66–85.
[15] A. Grothendieck, J.-L. Verdier, exposé IV of Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos, in: M. Artin, A. Grothendieck, J.-L. Verdier (Eds.), Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), in: Lecture Notes in Math., vol. 269, Springer, Berlin, New York, 1972.
[16] E. Howe, Isogeny classes of abelian varieties with no principal polarizations, in: G. van der Geer, C. Faber, F. Oort (Eds.), Moduli of Abelian Varieties, Texel Island, 1999, in: Progress in Math., vol. 195, Birkhäuser, Basel, 2001, pp. 203–216.
[17] A. Joux, R. Lercier, The Function Field Sieve in the Medium Prime Case, in: S. Vaudenay (Ed.), Advances in Cryptology — Eurocrypt 2006, in: Lect. Notes in Comp. Sci., vol. 4004, Springer, Berlin, 2006, pp. 254–270.
[18] A. Joux, R. Lercier, N. Smart, F. Vercauteren, The number field sieve in the medium prime case, in: C. Dwork (Ed.), Advances in Cryptology — CRYPTO 2006, in: Lect. Notes in Comp. Sci., vol. 4117, Springer, Berlin, 2006, pp. 323–341.
[19] T. Lange, Trace zero subvarieties of genus 2 curves for cryptosystems, J. Ramanujan Math. Soc. 19 (2004) 1–19.
[20] A.K. Lenstra, E.R. Verheul, The XTR public key system, in: M. Bellare (Ed.), Advances in Cryptology — CRYPTO 2000, in: Lect. Notes in Comp. Sci., vol. 1880, Springer, Berlin, 2000, pp. 1–19.
[21] J.S. Milne, On the arithmetic of abelian varieties, Invent. Math. 17 (1972) 177–190.
[22] B. Mazur, K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants, Ann. of Math. 166 (2007) 579–612.
[23] B. Mazur, K. Rubin, A. Silverberg, Twisting commutative algebraic groups, J. Algebra 314 (2007) 419–438.
[24] W.B. Müller, W. Nöbauer, Some remarks on public-key cryptosystems, Studia Sci. Math. Hungar. 16 (1981) 71–76.
[25] N. Naumann, Weil–Restriktion abelscher Varietäten, Diplomarbeit, Universität Essen, 1999.
[26] K. Rubin, A. Silverberg, Supersingular abelian varieties in cryptology, in: M. Yung (Ed.), Advances in Cryptology — CRYPTO 2002, in: Lect. Notes in Comp. Sci., vol. 2442, Springer, Berlin, 2002, pp. 336–353.
[27] K. Rubin, A. Silverberg, Torus-based cryptography, in: D. Boneh (Ed.), Advances in Cryptology — CRYPTO 2003, in: Lect. Notes in Comp. Sci., vol. 2729, Springer, Berlin, 2003, pp. 349–365.
[28] K. Rubin, A. Silverberg, Algebraic tori in cryptography, in: A. van der Poorten, A. Stein (Eds.), High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, in: Fields Institute Communications Series, vol. 41, AMS, Providence, RI, 2004, pp. 317–326.
[29] K. Rubin, A. Silverberg, Using primitive subgroups to do more with fewer bits, in: D. Buell (Ed.), Proceedings of Algorithmic Number Theory, 6th International Symposium, ANTS-VI, in: Lect. Notes in Comp. Sci., vol. 3076, Springer, Berlin, 2004, pp. 18–41.
[30] K. Rubin, A. Silverberg, Compression in finite fields and torus-based cryptography, SIAM J. Comput. 37 (2008) 1401–1428.
[31] J.-P. Serre, Complex multiplication, in: J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Thompson Book Co., Washington, DC, 1967, pp. 292–296.
[32] J.-P. Serre, Linear representations of finite groups, in: Graduate Texts in Mathematics, vol. 42, Springer, New York, 1977.
[33] J.-P. Serre, Cohomologie galoisienne, cinquième édition, révisée et complétée, in: Lecture Notes in Math., vol. 5, Springer, Berlin, 1994.
[34] A. Silverberg, Compression for trace zero subgroups of elliptic curves, Trends in Mathematics 8 (2005) 93–100.
[35] J.H. Silverman, The arithmetic of elliptic curves, in: Graduate Texts in Mathematics, vol. 106, Springer, New York, 1986.
[36] P.J. Smith, M.J.J. Lennon, LUC: A new public key system, in: E.G. Dougall (Ed.), Proceedings of the IFIP TC11 Ninth International Conference on Information Security IFIP/Sec '93, North-Holland, Amsterdam, 1993, pp. 103–117.
[37] P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, in: J. Pieprzyk, R. Safavi-Naini (Eds.), Advances in Cryptology — Asiacrypt 1994, in: Lect. Notes in Comp. Sci., vol. 917, Springer, Berlin, 1995, pp. 357–364.
[38] W.A. Stein, Shafarevich-Tate groups of nonsquare order, in: J. Cremona, J-C. Lario, J. Quer, K. Ribet (Eds.), Modular Curves and Abelian Varieties, in: Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 277–289.
[39] V.E. Voskresenskiĭ, Algebraic groups and their birational invariants, in: Translations of Mathematical Monographs, vol. 179, AMS, Providence, RI, 1998.
[40] A. Weil, Adeles and algebraic groups, in: Progress in Math., vol. 23, Birkhäuser, Boston, 1982.
[41] H.C. Williams, A $p+1$ method of factoring, Math. Comp. 39 (1982) 225–234.
[42] H.C. Williams, Some public-key crypto-functions as intractable as factorization, Cryptologia 9 (1985) 223–237.